Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 65 (2015) 853 – 858

Procedia Computer Science

International Conference on Communication, Management and Information Technology (ICCMIT 2015)

Security Issues Over Some Cloud Models

Passent M. El-Kafrawy[a], Azza A. Abdo[a], Amr. F. Shawish

Faculty of Science, Menoufia University, Menofia, Egypt
basant.elkafrawi@science.menofia.edu.eg

Abstract

Cloud computing is an uprising field in information technology (IT) industry because of its performance, high availability, low cost and much more. The data leakage, lack of proper security control policy, and weakness in the data sentry are the main worries of the companies. So that a cloud data security models should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated. This paper focuses on two phases; the first phase is a discussion of the security functions that should be realized during building any data cloud model. A comparison of some designed cloud models is discussed as the second phase. The cloud models discussed are Wang scheme (2009), Prased scheme (2011), Sandeep K. Sood (2012), Xin Dong scheme (2014), and P. Lavanya scheme (2014) all of which are displayed and its security are discussed. A discussion of a number of possible security measures is our concern in this paper, which should be considered in any cloud based model. Recommendations are further given for proper security issues over cloud systems.

Peer-review under responsibility of Universal Society for Applied Research

Keywords: Cloud computing, Security factors

1. Introduction

As a matter of fact IT is a set of tools, methodologies, and tasks with the required equipment to collect, process, and provide information. Generally, speaking, IT is used for office automation, multimedia, and telecommunication. IT challenges are, Globalization, Aging Data Centers, Storage Growth, Application Explosion, Cost of ownership and

Peer-review under responsibility of Universal Society for Applied Research
doi:10.1016/j.procs.2015.09.041

Acquisitions. The IT challenges have made organizations think about the Cloud Computing model to provide better service to their customers. Cloud computing is internet-based computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Cloud computing generally has five characteristics: rapid elasticity, measured service and on-demand self-service: resources can be provisioned via automated mechanisms [1]. There are four common deployment models for cloud services loosely determined by who has access to the cloud services: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud [2]**. Cloud computing security** or, more simply cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing [3].

The data leakage, lack of proper security control policy, and weakness in the data sentry are fears of the companies. So that cloud data security models should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated.

Moving applications to the cloud and accessing the benefits means first evaluating specific data security issues and cloud security issues**.** When companies move applications from on-premise to cloud-based, challenges arise from data residency, industry compliance requirements, privacy and third party obligations concerning the treatment of sensitive data. Corporate policies or the regulations of the governing jurisdictions impact the way sensitive data is managed including where it is located, what types of data can be collected and stored and who has access to it. These issues can determine the degree to which organizations can realize the value of cloud computing. Cloud security issues fall primarily into three areas: **1- Data Residency** - Many companies face legislation by their country of origin or the local country that the business entity is operating in, requiring certain types of data to be kept within defined geographic borders. There are specific regulations that must be followed, centered around data access, management and control. **2- Data Privacy** - Business data often needs to be guarded and protected more stringently than non-sensitive data. The enterprise is responsible for any breaches to data and must be able to ensure strict cloud security in order to protect sensitive information. **3- Industry & Regulation Compliance** - Organizations often have access to and are responsible for data that is highly regulated and restricted. Many industry-specific regulations such as GLBS, CJIS, ITAR and PCI DSS, require an enterprise to follow defined standards to safeguard private and business data and to comply with applicable laws. Cloud computing security issues include preserving confidentiality and privacy of data, authorization, authentication and integrity. We shall investigate some security functions to solve security issues on the cloud.

This paper focuses on two phases; the first phase is a discussion of the security functions that should be realized during building any data cloud model to cover security issues. A comparison of some designed cloud models are discussed as the second phase. In this paper, the five algorithms Wang's scheme (2009) [7], Prased's scheme (2011) [9], Sandeep K. Sood (2012) [10], P. Lavanya's scheme (2014) [11] and Xin Dong's scheme (2014) [12] are described. Also we analyze these five algorithms focusing on the security factors defined in section 2. In addition to these factors, we put additional factors such as scalable data sharing, privacy, fake identity and balance security and usability, which will be defined in section 4 as requirements for secure cloud systems.

This paper is designed as following, Section 2 illustrates the security functions over cloud computing. Section 3 related work on the cloud models. Comparison of algorithms is presented in Section 4. Finally conclusion is given in in section 5.

2. Security functions over cloud computing

An efficient cloud data security model should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing to reach its maximum heights and propel in the direction it is designed for, by preventing the owner's data from all the risks associated and gives for cloud model more security and efficiency. The security functions over cloud computing are listed as following:

Table 1. Security Functions

Identification and authentication:	The role of identity and authorizations management is to ensure that only authorized persons may use the IT resources. Access to all the IT systems or services must be made secure by identifying and authenticating the users seeking access to IT systems. [4]
Authorization:	The particular access level of the authorized user.
Confidentiality:	Where and how the data is stored. This includes the security of the data storage application, operating system, and any other applications that may be running on the same system as well as the physical storage location [5].
Non-repudiation:	Any access to customer data is logged.
Integrity:	Data integrity is defined as the accuracy and consistency of stored data, in absence of any alteration to the data between two updates of a file or record. Cloud services should ensure data integrity [6].
Encryption:	Is the process of converting data to a form which cannot be used in any meaningful way without special knowledge and the process of converting the encrypted data back to its original form is called decryption.
Storage provider verification:	Verifying of these storage providers which people and organizations buy to store their data.
Secure even after loss of user identity and password.	Secure even after loss of user identity and password.
Indexing of data:	To reduce the amount of data transferred inside the Cloud, and facilitates the deployment of database back-end applications.
Keyword search:	A type of search that looks for matching documents that contain one or more words specified by the user.

3. Related Work

A Pseudorandom Data verification scheme was proposed by Wang and et al (2009). The scheme verifies the storage correctness of user data in cloud **[7].** Wang and et al scheme achieves the guaranty of data availability, reliability and integrity. However, this scheme was also not providing complete protection to user data in cloud computing, since pseudorandom data would not cover the entire information.

In 2010, S. Kamara et al. [8] proposed a security scheme for customers to store and share their sensitive data in the cloud storage. The scheme provides a basic encryption and decryption mechanism for providing security. In S. Kamara scheme, when a user wants to send data to another user, they first generate a master key that encrypts their message. The secret key for decryption is stored on receivers' system for decrypting the same message. They used the concept of index encryption and tokens that are generated with the knowledge of secret key. The searching method is not very efficient for encrypted data. The symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE) are used in the scheme to encrypt data searching, but this techniques increase complexity and make the system slow. In 2011, Prasad et al discussed different security aspects in cloud computing [9], this technique provides a way to authenticate in a 3-dimensional approach. In this scheme, the data classification is done by a client before storing the data. The client who wants to send the data for storage needs to give the values C (confidentiality), I (integrity), A (Availability). The value of C is based on level of secrecy at each junction of data processing and prevents unauthorized disclosure, value of I based on how much assurance of accuracy is provided, reliability of information and unauthorized modification is required, and value of A is based on how frequently it is accessible. Accordingly data having the higher rating is considered to be critical and 3D security is recommended on that data. According to the concept of 3D, a user who wants to access the data need to be authenticated, to avoid impersonation and data leakage. Now there is a third entity who is either company's (whose data is stored) employee or customer who wants to access, they need to register first and then before every access to data his/her identity is authenticated for authorization. But in this model, the data stored is not in encrypted form and once the username and password is

lost, the data can easily be retrieved by any unauthorized user.

In 2012, Sandeep K. Sood discussed, a framework comprising of different techniques and specialized procedures that can efficiently protect the data from the beginning to the end, from the owner to the cloud and then to the user [10]. The proposed model has been structured by bringing together various techniques and utilizing them to perform the task of data security in cloud. This combination of diverse methods operate as a wall stood together against the security challenges, which have been constantly creating the loop holes in the efficient functioning and growth of the cloud.

In 2014, P.lavanya and et al [11], Xin Dong and et al [12] proposed two models for data sharing over cloud computing. A secure multi-owner data sharing scheme, for dynamic group in the cloud, was proposed by P. Lavanya et al. The scheme proposed a One-Time Password, which is one of the easiest and most popular forms of authentication that can be used for securing access to accounts. A user is able to share data with others in the group without revealing identity privacy to the cloud.

Xin Dong et al. proposed a data sharing, fueled by favorable trends in cloud. It is emerging as a promising technique for allowing users to conveniently access data. Xin. Dong's scheme focuses on providing a dependable and secure cloud data sharing service that allows users dynamic access to their data. A privacy-preserving data policy with semantic security is proposed in the scheme; by utilizing cipher text policy attribute-based encryption (CP-ABE) combined with identity-based encryption (IBE) techniques.

4. Comparison (Models Evaluation)

In this section, a comparison between the algorithms Wang's scheme (2009) [7], Prased's scheme (2011) [9], Sandeep K. Sood (2012) [10], P. Lavanya's scheme (2014) [11] and Xin Dong's scheme (2014) [12] is described. We analyze these five algorithms focusing on the security factors defined in sec.2. In addition to these factors, we put additional factors such as **Scalable Data sharing, Privacy**, **Fake identity** and **Balance security and usability.**

These factors are defined as in the following table.

Table 1. Additional Security factors

Scalable Data sharing:	There is now a growing focus on implementing scalable data sharing capabilities in the Cloud. With the ability to share scalable data via the Cloud.
Privacy:	Privacy is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights and the European Convention on Human Rights [13].
Fake identity	Authorized users reveal their passwords to unauthorized users [14].
Balance security and usability	Security and usability are often contradictory. To make a system secure, you have to introduce checks that users are authorized to use the system and that they are acting in accordance with security policies [14].

Table 3: Security models Comparison.

	Wang' scheme (2009)	***Prased' scheme (2011)***	***Sandeep K. Sood (2012)***	***Xin Dong scheme (2014)***	***P. Lavanya scheme (2014)***
Identification and authentication	Yes	Yes	Yes	Yes	Yes
Authorization	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes		
Non-repudiation	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes

Encryption	No	No	Yes	Yes	
Storage provider verification	No	No	Yes	Yes	Yes
Secure even after loss of user identity and password	No	No	Yes	Yes	Yes
Indexing of data	No	No	Yes	Yes	Yes
Keyword search	No	No	Yes	Yes	Yes
Scalable Data sharing	No	No	Yes	Yes	Yes
Privacy	Yes	Yes	Yes	Yes	Yes
Fake identity	No	No	No	No	No
Balance security and usability	No	No	No	No	No

In table 3, we compared between some cloud models according to the previously discussed security functions such as: Identification and authentication, Authorization, Confidentiality, Non-repudiation, Integrity, Encryption, Storage provider verification, Secure even after loss of user identity and password, Indexing of data, Keyword search, Scalable Data sharing, Privacy, Fake identity and Balance security and usability. **Wang's scheme (2009) [7]** handled some security issues such as Identification and authentication, Authorization, Confidentiality, Non-repudiation, Integrity and Privacy but there are some security issues in this model not solved such as Encryption, Storage provider verification, Secure even after loss of user identity and password, Indexing of data, Keyword search, Scalable Data sharing, Fake identity and Balance security and usability. **Prased's scheme (2011) [9]** had not added any thing new to the **Wang's scheme (2009) [7]** where it treated the same security issues and it didn't solve any problems in the previous model**.**

Sandeep K. Sood (2012) [10], P. Lavanya's scheme (2014) [11] and Xin Dong's scheme (2014) [12] solved some security issues that was unresolved in the previous schemes such as Encryption, Storage provider verification, Secure even after loss of user identity and password, Indexing of data, Keyword search, Scalable Data sharing. But some security issues were not solved in these schemas such as Fake identity and Balance security and usability.

Xin Dong's scheme (2014) [12] provided a dependable and secure cloud data sharing service that allows users dynamic access to their data, ensuring robust data sharing security, provide an adversary model, as previously described, with a secure, private and scalable policy for data sharing in cloud computing, ensure the overheads of the service provided by the system and is as light as possible. The scheme ensures fine-grained data access control, backward secrecy and security against collusion of users with the cloud. The disadvantage is when authorized users reveal their passwords to unauthorized users. In this case the unauthorized users can access the stored data (information) on the cloud and possible tamper, update and delete any information in the cloud. Thereby reducing the security level in the whole system. This model is very important and can be considered s a base for future work to achieve higher security.

Many factors influencing the raise of capabilities of cloud computing to solve security issues was identified in the previous table. Wang's scheme (2009) [7] and Prased's scheme (2011) [9] enforced some factors of security such as *Identification and authentication*, *Authorization*, *Confidentiality*, *Non-repudiation* and *Integrity* but some factors yet to be solved such as *Encryption, Storage provider verification*, *Secure even after loss of user identity and password*, *Indexing of data* and *Keyword search*. Sandeep K. Sood (2012) [10] solved some other factors such as *Encryption, Storage provider verification*, *Secure even after loss of user identity and password*, *Indexing of data* and *Keyword search*. P. Lavanya's scheme (2014) [11] and Xin Dong's scheme (2014) [12] are the most schemas covering security issues because they achieved the previous factors in addition to *Scalable Data sharing and Privacy.* But many problems yet to be solved in all previous schemes such as fake identity and balance security and usability, which shall be addressed in future research.

5. Conclusion and future work

A cloud data security models should be able to overcome all the data security, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated. This paper illustrated the security functions that should be realized during building any data cloud model to cover most security issues and concerns. Also a comparison of some designed cloud models was discussed. Our contribution of this paper is a discussion of a number of possible security measures, which should be considered in any cloud based model. As future work, a cloud data model covering all security functions, which are mentioned at this paper, shall be proposed.

References

1. P. Meld, and T. Grance, "The NIST definition of cloud computing," NIST special publication 800-145, September 2011.
2. P.G. Patel, and S.M. Shah "Survey on Data Security in Cloud Computing "In International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 9, November- 2012 ISSN: 2278-0181.
3. P.Kr.Verma, and J.Shekhar "Data Protection Issues in Cloud Computing "In 2'nd International Conference on Role of Technology in Nation Building, ICRTNB-2013.
4. Michael Hange," "Security Recommendations for Cloud Computing Providers (Minimum information security requirements)",In White Paper, Section 114, Security Management and IT- Grundschutz, P.O. Box 20 03 63, 53133 Bonn, 2011.06.22.
5. A. Hudic, S. Islam, P. Kieseberg, S. Rennert and E.R. Weippl "Data confidentiality using fragmentation in cloud computing "In International Journal of Pervasive Computing and Communications, Vol. 9 No. 1,pp. 37-5, 2013.
6. Venkatesa Kumar V and Poornima G," Ensuring Data Integrity in Cloud Computing "In Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-4, and February 10, 2012.
7. Wang C, Wang Q, Ren K, Lou W" Ensuring data storage security in cloud computing"In quality of service, 2009, IWQoS IEEE 17th international workshop, p. 1–9, 2009.
8. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
9. Prasad P, Ojha B, Shahi RR and Lal R" 3-dimensional security in cloud computing "In Computer Research and Development (ICCRD), 2011 3rd International Conference on ,2011.
10. Sandeep K. Sood," A combined approach to ensure data security in cloud computing", In Journal of Network and Computer Applications 35 (2012) 1831–1838.
11. P Lavanya, S Komala and N Vikram "Anonymous Data Sharing Scheme for Dynamic Groups in an Untrusted Cloud", IPASJ International Journal of Computer Science (IIJCS), Volume 2, Issue 8, August 2014.
12. Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue and Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing "In journal of computer & security xxx (2014) I-14.
13. Siani Pearson," Taking Account of Privacy when Designing Cloud Computing Services "In HP Laboratories, HPL-2009-54, March 6, 2009.
14. Ian Sommerville," Software engineering — 9th" ed. p. cm. ISBN-13: 978-0-13-703515-1, ISBN-10: 0-13-703515-2, 2011.